

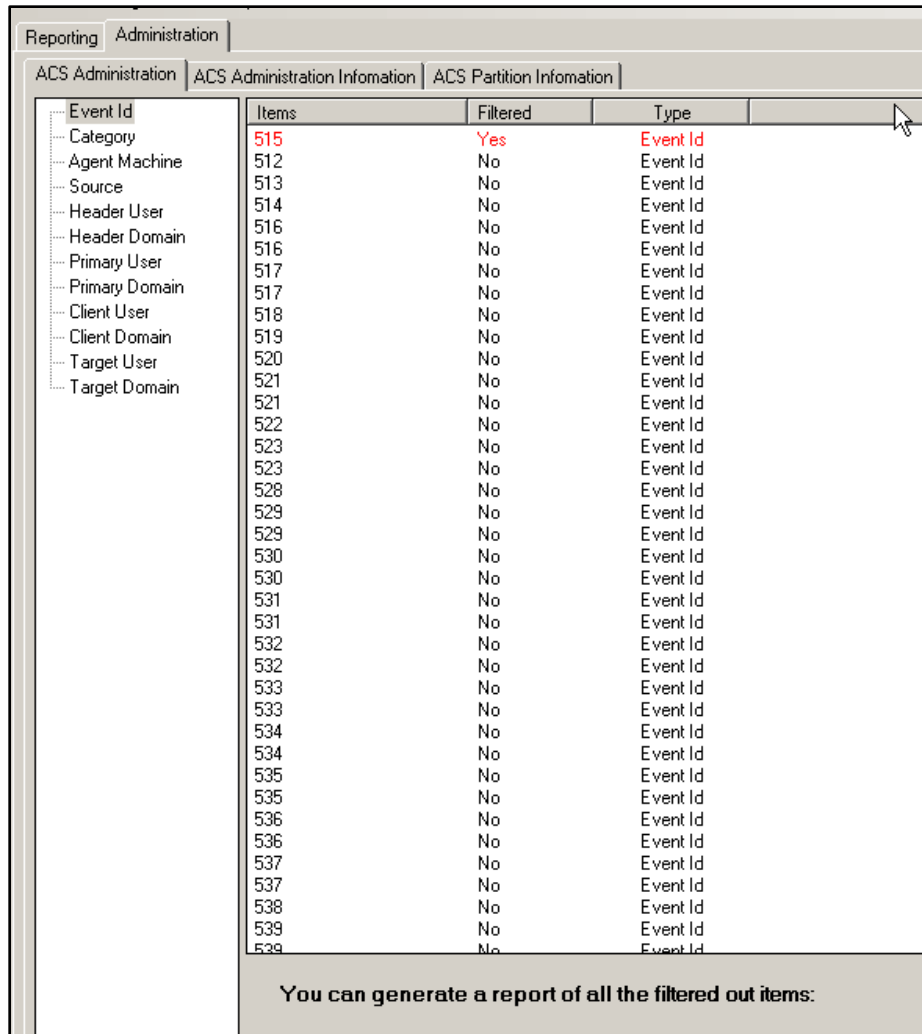
ACS EVENT FILTER MANAGER

Administration Console

A significant administrative task is to review and decide which events and parameters are to be removed from the standard collection activity. This decision should be made with organizational and industry best standard in mind. Each organization has unique requirements as to the collection and retention of event and parameter data. There exists potential liability in not collecting all events. However, in practice, some events and parameter may be redundant and have little or no value. After careful consideration, event reduction is often warranted.

The eSCOP Event Filter Manager is designed to provide an easy method for view and managing events and parameters. Once a decision has been made to eliminate an event or parameter, the Event Filter Manager provides a point and click interface to remove the item(s) for normal collection. To complete the process, the ACS service will need to be restarted to assure proper dissemination of the instructions.

For example, in a given environment, it may be determined that some of the possible Access Enforcement rule events are deemed unimportant. In this case, the system administrator would use the eSCOP Event Filter Manager to disable the collection of non-essential events. In another example, specific servers within a domain may provide non-mission critical functions and therefore does not warrant audit collection. In this case, the system administrator would add the designated system/device to the items to be filtered out of the collection process.



The screenshot shows the Administration Console of the ACS Event Filter Manager. It features a navigation pane on the left with a tree view containing 'Event Id', 'Category', 'Agent Machine', 'Source', 'Header User', 'Header Domain', 'Primary User', 'Primary Domain', 'Client User', 'Client Domain', 'Target User', and 'Target Domain'. The main area displays a table with columns for 'Items', 'Filtered', and 'Type'. The 'Items' column lists event IDs from 512 to 539. The 'Filtered' column shows 'Yes' for event ID 515 and 'No' for all other event IDs. The 'Type' column lists 'Event Id' for each row. A mouse cursor is visible over the table. At the bottom of the console, a message states: 'You can generate a report of all the filtered out items.'

Event Id	Items	Filtered	Type
512	512	No	Event Id
513	513	No	Event Id
514	514	No	Event Id
516	516	No	Event Id
516	516	No	Event Id
517	517	No	Event Id
517	517	No	Event Id
518	518	No	Event Id
519	519	No	Event Id
520	520	No	Event Id
521	521	No	Event Id
521	521	No	Event Id
522	522	No	Event Id
523	523	No	Event Id
523	523	No	Event Id
528	528	No	Event Id
529	529	No	Event Id
529	529	No	Event Id
530	530	No	Event Id
530	530	No	Event Id
531	531	No	Event Id
531	531	No	Event Id
532	532	No	Event Id
532	532	No	Event Id
533	533	No	Event Id
533	533	No	Event Id
534	534	No	Event Id
534	534	No	Event Id
535	535	No	Event Id
535	535	No	Event Id
536	536	No	Event Id
536	536	No	Event Id
537	537	No	Event Id
537	537	No	Event Id
538	538	No	Event Id
539	539	No	Event Id
539	539	No	Event Id

You can generate a report of all the filtered out items:

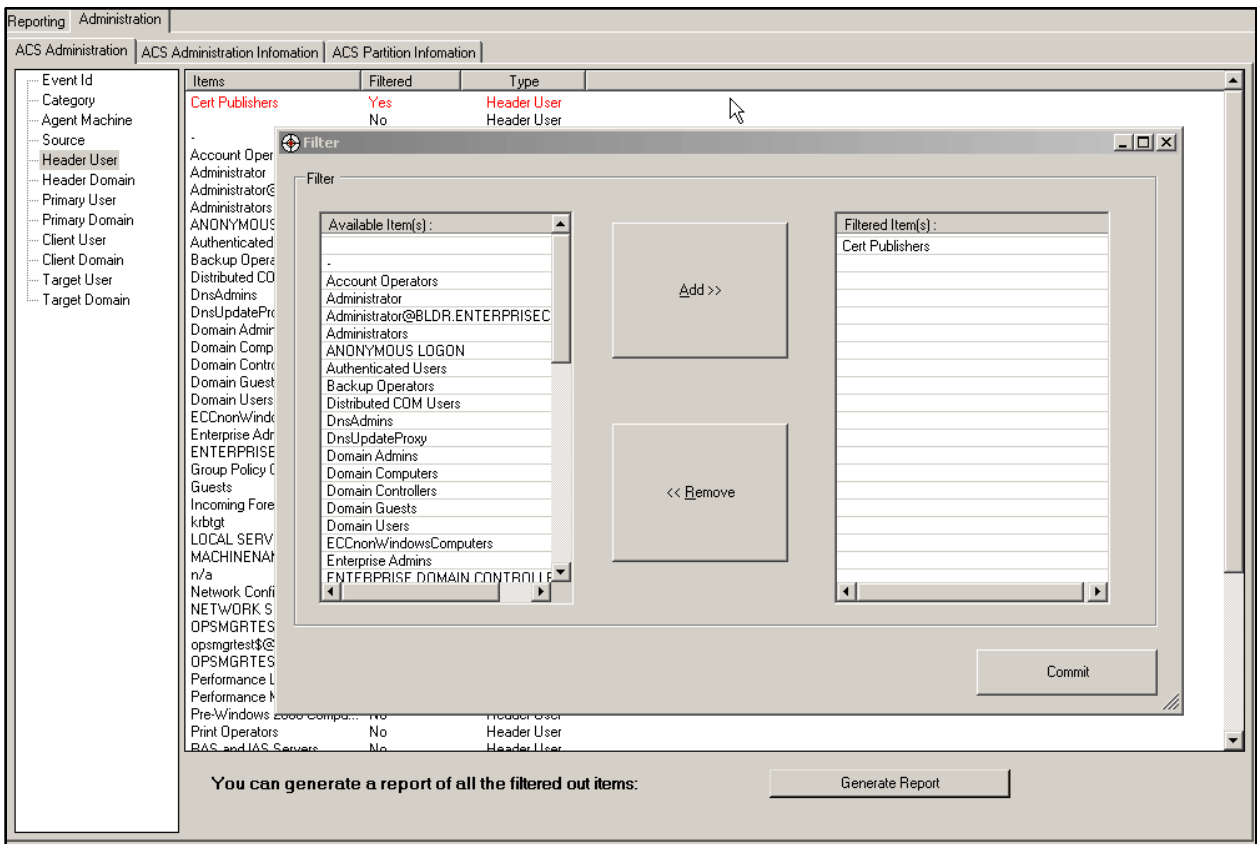
The eSCOP Event Filter Manager Console provides a list of current events and parameters that are being collected. The right column lists the event and parameter categories. By clicking on an item, the right window expands to provide the detail individual events and parameters.

The eSCOP Administrative Sub-Console permits the management of a wide number of parameters including

- Event Identification – Individual events may be selected and added to list of filtered-out items
- Category – Major parameter category filtering is provided based upon the following:
 - System Event
 - Logon/Logoff
 - Object Access
 - Privilege Use
 - Detailed Tracking
 - Policy Change
 - Account Management
 - Directory Service Access
 - Account Logon
- Agent Machine – Filtering is provided based upon agent status criteria
- Source – Filtering is provided based upon the source
- ACS Source – Filtering is provided based upon the specific ACS sources:
 - Microsoft Windows Security Auditing
 - Security
 - Others
- Header User – Filtering is provided based upon the header user criteria:
 - Computer
 - System
 - Administrator
 - Local Service
 - Network Service
 - Anonymous Logon
 - Owner
 - Other
 - Not Applicable
- Header Sid – Filtering is provided based upon the header system identification
- Header Domain – Filtering is provided based upon the header domain criteria
- Primary User – Filtering is provided based upon the primary user
 - Computer
 - System
 - Administrator
 - Local Service
 - Network Service
 - Anonymous Logon
 - Owner
 - Other
 - Not Applicable
- Primary Sid – Filtering is provided based upon the primary system ID
- Primary Domain – Filtering is provided based upon the primary domain
- Client User – Filtering is provided based upon the client user

- Computer
 - System
 - Administrator
 - Local Service
 - Network Service
 - Anonymous Logon
 - Owner
 - Other
 - Not Applicable
- Client Sid – Filtering is provided based upon the client system ID
 - Client Domain – Filtering is provided based upon the client domain
 - Target User – Filtering is provided based upon the target user
 - Target Sid – Filtering is provided based upon a target system ID
 - Target Domain – Filtering is provided based upon a target domain
 - Primary Logon Id – Filtering is provided based upon a primary logon ID
 - Client Logon Id – Filtering is provided based upon a client logon ID

In order to select an event or parameter for collection removal, right click on primary category and selection Filter ... the management interface is then displayed. Highlight the desired item, select ADD button to place the item on a do not collect list. To later begin collection on the item again, simply use the same interface to REMOVE it from this list.



Finally, restart the ACS service in order to assure dissemination of the new collection rules.